Counter Bio-Terror

Peter Garretson

The author is a Visiting Fellow at IDSA, New Delhi.

Summary

There is much more to a whole of government response to a bio-terror attack than the public health system. For adequate government performance in such an emergency, and to directly counter terrorist goals of instilling panic and undermining the government, many additional capabilities must be exercised. Because a bio-terror response involves so many different agencies, it is also a rich forum for bilateral cooperation, as it multiplies the strategic touch-points between nations and leads to more robust and timely communication and response with good cross-domain learning.

Modern Nation States are complex systems that today suffer from the affliction of terrorism, which can attack its vital centers and connective tissue. Even as nation's try to counter, terrorists are themselves evolving and seeking new capabilities to more effectively injure their hosts, including all forms of weapons of mass destruction (WMD).

While there is a general worrisome trend of proliferation of WMD-related skills and tools, nowhere are the barriers to entry coming down faster than in the field of biological weapons. The worldwide boom in biotechnology has proliferated biotechnology expertise world wide, while world wide web, and flattening of the world means the same pool of information, talent, and capital is also available to those who oppose the existing order.

Whereas once the full resources of a nation-state were required for a bio-weapons program, this is no longer the case. Although ultimately unsuccessful in weaponization, as far back as a decade ago, Aum Shinrikyo[1], a sub-national group showed it had both the intent and capability to procure such capabilities and expertise. Since then, the precursors, data, expertise, equipment, and finances are all much more available.

For a long time, policy makers have taken comfort in the knowledge that dangerous pathogens were kept under lock and key in controlled facilities. But this is no longer the case.

With the advent of on-line catalogs of gene sequences, the proliferation of low-cost, portable gene sequencers, mail-order sequences, and the rapid advances in synthetic biology, researchers have proven that they can manufacture pathogens "ex-nihili." This creates the worrisome possibility in the not too distant future of genetic "hackers" creating designer pathogens in a computer and then hitting "print" to their local gene sequencer. As with 9-11, we are confronted with the capability of malcontents to use our own tools against us.

Countering such capabilities and low signature activities will be difficult. Countering them

in liberal, pluralist democracies like India and the US will be doubly challenging, as we value the diversity of thought and discourse and are hesitant to suppress dissent or heavily indoctrinate our citizenry into a single view of "the good."

But we must not fail to evolve our own immune systems, and one thing states can do is band together to ensure dissemination of best practices and ability to lend mutual support.

As a necessary consequence with violent intent have greater freedom to speak, spread, connect, travel and operate. We cannot suppress. Instead, we must evolve and adapt our immune systems.

The core of any response to bio-terrorism is excellence in one's Public Health System. Only the ability to contain and respond to an outbreak of a disease can limit its damage.

Proactive development of a responsive Public Health System is necessary, but not sufficient. There is an urgent need to address the Non-Public Health aspects of Counter-BioTerrorism (C-BT), but these are not well understood.

In general, the Non-Public Health aspects of Counter Bio Terror include state policies and actions that might prevent a bio-terror attack, state posture to deny the benefits and attractiveness of an attack, actions to be taken by non-public health agencies in coping with and responding to an attack, attribution forensics, and potential state responses to the perpetrators of an attack.

Prevention

There are a number of policies and actions states can take that can help prevent an attack from ever occurring. First is active construction of Arms Control regimes that dissuade states from undertaking bio weaponization programs that directly proliferate offensive knowledge, and tools that might fall into terrorist hands. Second is the construction of international criminal norms and cooperative mechanisms for handling non-state actors engaged in bio-terror schemes and actions. This might include the shaping of existing bodies such as the role of the International Criminal Court, or constructing new bodies, such as an INTERPOL for Asia. Third is the development of norms relating to States taking legitimate self defense against sub-national actors within their own borders and against actors in another's sovereign territory when they are not able or willing. Fourth is putting in place cooperate agreements that aid in bio-forensics where the expertise may lie outside of public health agencies. And finally, selective intelligence sharing agreements that facilitate prevention, attribution, and response.

Posture

A second non-public health aspect of C-BT is a state posture to deny the benefits and attractiveness of an attack. The first action states can take to deter action is to have explicitly stated response policies that give both terrorists and would be state sponsors pause. States should decide in advance how they wish to counter, whether it be with ambiguity or clear red lines that if crossed, would engender a very serious response. A second aspect involves making the freedom of maneuver of the terrorists in society more difficult, but creating public awareness about what constitutes suspicious activity and to whom to report it. The final and most important aspect is defence by denial, meaning that the posture of the state is such that an attack will not have its intended impact. A terrorist attack is usually demonstrative act intended to communicate some message to a particular audience, either to force some capitulation based upon a power of blackmail/threat, or weaken and erode the existing order by demonstrating its weakness in order to ultimately replace it with something else, or by provoking an over-reaction by the government or some partisan group which further undermines societal bonds for the same end. In either case, the terrorist looks to make the state look inept and helpless, and to make itself look powerful, and uncounterable. To that end, it seeks to maximize the psychological impact by maximizing damage and casualties and the ineptitude of the state in prompt response, and the presence of both in the media reaching its chosen audience. Here the state can deny such benefits by having a well orchestrated

and exercised inter-agency response with strong strategic communications capability. This involves such matters as civil defence plans, stocks of agent response medicines, and having conducted detailed response exercises involving all relevant departments and agencies based on multiple scenarios to iron out interagency responsibilities and communication bottlenecks.

Coping

Another aspect that must be considered is the actions taken by non-public health agencies in coping with and responding to a bio-attack. A bio-terror attack will be different from a more ordinary disease outbreak in that it will require coordination, and command and control of non-public health responder teams, including special capabilities resident in law enforcement, intelligence, military units. States must consider the necessary strength, training, and equipage of such teams for such functions as surveillance, response, and decontamination, as well as how they interact with one another and who has lead authority and jurisdiction in which phase, and where they should reside in the overall command and control concept.

A second aspect of coping involves the creation and maintenance of national level tools for consequence modeling, decision-making, graphic outputs for public communication and inter-agency collaboration, command & control. There is a need to ensure that key decision-makers have access to high quality tools that allow them to make the best possible decisions and inputs to the public response infrastructure in the minimum amount of time. Such tools would be grounded in an overall Geographic Information System with population densities, location of critical infrastructure, traffic flow and congregation patters, that can accept meteorology, model plume distribution, epidemiological models, infection/contagion response curves, and analytic tools to make evacuation and quarantine decisions.

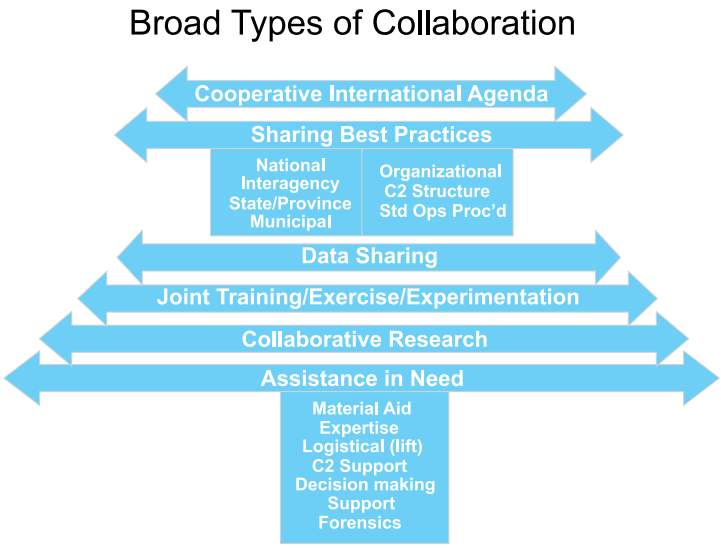
Attribution

Another aspect of a whole-of-government counter-bioterror effort likely to involve capabilities outside the public health structure is attribution forensics. There is a need for policies and procedures that address the role of intelligence, law enforcement, and military research and bio-weapons experts and related labs in the effort in post-attack forensics and attributions. There is a need to specify at what point authority shifts from first responders to forensics, and how intelligence, law enforcement, and military capabilities cooperate and share information, including the leveraging of other nation's intelligence, law enforcement, and military expertise and non-overlapping knowledge.

Response

Another area which differentiates a natural disease from a bioterror attack is the state response against the state actors or non-state actors and their sponsors after attribution. This may or may not require a declarative policy. For a state actor, it might require clarity (at least internally) as to whether or not it would generate a conventional response, sub-conventional response, and in-kind response, a nuclear response, and degree of desired ambiguity. Whether or not a stated policy exists, it is useful to run through scenario planning to have thought through what is and is not actionable, and at what would be the triggers (of kind, of severity) for such action.

Collaboration



India and the United States, with large populations and population densities, high amounts of international traffic, and open democratic systems share concerns about their permeability to terrorist attacks. Counter-Bio Terror is an attractive area for meaningful Indo-US bilateral security collaboration.

Some might balk at the magnitude of the problem of coordinating so many different agencies, particularly given the extremely limited cross-bureaucracy dialogue and bandwidth below the most senior levels, but seen in this light, "it is not a bug, it is a feature." As discussed above, any response to counter-bioterror would be tremendously interdisciplinary and inter-agency, fraught with interesting and difficult command, control, and cooperation problems, which require a wide number of contacts involved, both at the C2 and technical expertise levels, at central, state, and local levels. By thinking through together counter-bioterror scenarios, significant mutual learning is likely to take place, including sharing of best practices.

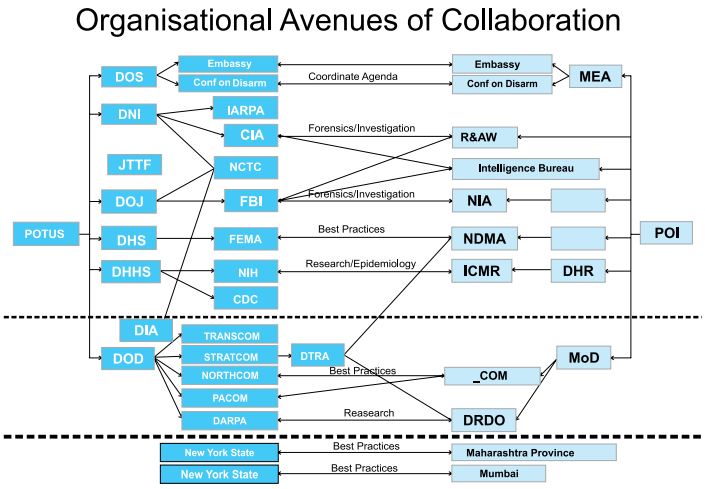
The organisational learning from such a rich scenario is likely to result in significant cross-domain learning, and useful transfer to other counter-terrorism efforts, including other Weapons of Mass Destruction (WMD), such as nuclear or chemical, and other Weapons of Mass Effect (WME), such as cyber attacks, and natural or man-made accidental catastrophes (Earthquake, Tsunami, Typhoon, Nuclear or Chemical accident).

Paths To Cooperation

If counter-bioterror is a rich topic for bilateral cooperation, what might it look like? There are two general categories, both of which allow for reduced time time lag and increased effectiveness in preventing and coping. The first deals with proactive measures, and the second with reactive measures.

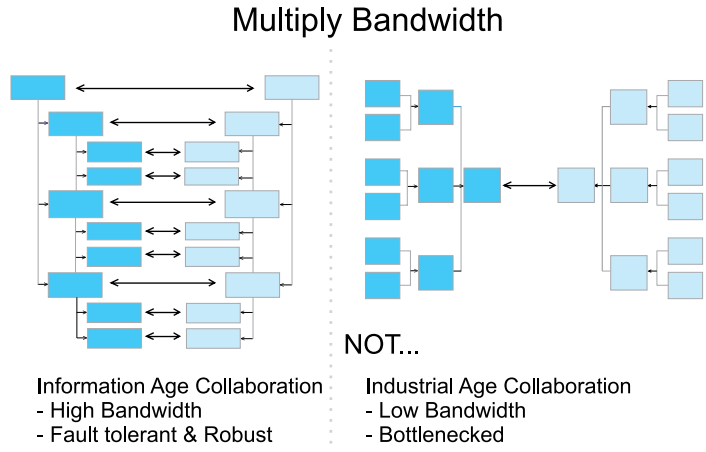
Proactive Collaboration

Typically there is some parallel or equivalent organisation in each country that needs to be talking about non-sensitive matters below the



Joint Secretary level, to be aware of each other's capabilities and challenges.

Such organisational touch-points typically relate to those serving some command and control function (who is tasked, how, what procedures are followed, who takes decisions), and those with expertise particular to the function they serve (forensic expertise, investigative expertise, etc.).



By proliferating the contacts between domain expertise and command & control structures the number of possible data-flows increases, reducing the chance of a "strategic bottleneck," and allowing for rapid response reactions and high bandwidth information flow in an actual emergency. In all cases, it is useful to understand each other's best practices and consider internal reform as well as consideration for the actual limitations of the other side. In some cases, data sharing agreements between like organisations can speed detection, characterization, forensics, and response. In other cases, there may be

opportunities to do collaborative research, such as work on new means of detection, characterization, and agent countering, or decision-making tools. And in some cases, as with first responders, joint training, exercises, and experimentation are very useful in closing the seams between organisations that are not used to working together and understanding the previewing of problems likely to arise in interaction, so as to find work around. Another useful area for collaboration is in compatibility between decision support software suites to allow sharing of data, models, and remote reach-back support.

A final area for collaboration is setting a cooperative international agenda to set norms, counter the potential use, and make bio-weapons proliferation more difficult.

Reactive Collaboration

This category generally refers to becoming familiar with material assistance the other country is capable of providing in an hour of need. Such assistance might include material aid (medicines, decontamination gear, tents, blankets, water, etc.), expertise (medical, investigative, forensic), and specialized packaged capabilities, such as logistical support, air and sea lift, decontamination teams, counter-terrorism units, deployable forensic experts, remote sensing / biosensor kits, and command, control and communications (C3) capabilities. Typically such requests for assistance are worked through the respective embassies, but receiving organisations must understand in advance what are the menu of options they can request in order to even think about requesting them. Likewise, it is useful for them to have some familiarity with the organisation providing the assistance, and the realistic capabilities and timeframes from request to deployment. Sometime there are established alternate channels (such as Air Force, Navy, Army, and theater combatant command dialogues), which could be used to good effect.

Endnotes:

1 Kaplan, David E., The Cult at the End of the World: The Terrifying Story of the Aum Doomsday Cult, from the Subways of Tokyo to the Nuclear Arsenals of Russia (Hardcover), 1996.